1-1-2017

Biometrics: The Future is in Your Hands

Kelsey Sherman
Loyola Law School, Los Angeles

BIOMETRICS: THE FUTURE IS IN YOUR HANDS

*Kelsey Sherman**

I. INTRODUCTION

In September 2016, Yahoo confirmed that data associated with at least 500 million user accounts had been stolen in 2014, making Yahoo and its users victims of one of the largest cybersecurity breaches of all time.[1] Based on public disclosures, it is estimated that "[between 2004 and 2014], there [were] over 300 data breaches involving the theft of 100,000 or more records."[2] Such breaches are only likely to increase going forward.[3] It is estimated that, by 2025, "approximately 80 billion devices will be connected to the [i]nternet," and that "the total amount of digital data created worldwide will . . . hit 180 zettabytes."[4]

Yahoo, in response to the breach, rolled out a new security upgrade for its e-mail application based on biometrics.[5] This upgrade allows users to scan their fingerprints as a password to access their inbox.[6] Using biometrics as an additional security feature is changing

* J.D. Candidate, May 2018, Loyola Law School, Los Angeles; B.A., English, Georgetown University in Washington, D.C. Thank you to Professor Karl Manheim for his guidance and encouragement, and to my family for their love and support.

1. Seth Fiegerman, *Yahoo Says 500 Million Accounts Stolen*, CNN (Sept. 23, 2016, 10:39 AM), http://money.cnn.com/2016/09/22/technology/yahoo-data-breach.

2. Niall McCarthy, *Chart: The Biggest Data Breaches in U.S. History*, FORBES (Aug. 26, 2014, 8:17 AM), http://www.forbes.com/sites/niallmccarthy/2014/08/26/chart-the-biggest-data-breaches-in-u-s-history/#35228b585ead.

3. Elsie Viebeck, *FBI: Data Breaches 'Increasing Substantially'*, HILL (May 14, 2015, 3:01 PM), http://thehill.com/policy/cybersecurity/242110-fbi-official-data-breaches-increasing-substantially.

4. Michael Kannellos, *152,000 Smart Devices Every Minute In 2025: IDC Outlines The Future of Smart Things*, FORBES (Mar. 3, 2016, 6:25 PM), https://www.forbes.com /sites/michaelkanellos/2016/03/03/152000-smart-devices-every-minute- in-2025-idc-outlines-the-future-of-smart-things/2/#35c8dc9b71c4. For an explanation of the size of a zettabyte, see Charles Arthur, *What's a Zettabyte? By 2015, The Internet Will Know, Says Cisco*, GUARDIAN (June 29, 2011), https://www.theguardian.com/technology/blog/2011/jun/29/zettabyte-data-internet-cisco.

5. *Yahoo Adds Fingerprint Security After Massive Hack*, PLANET BIOMETRICS (Sept. 26, 2016, 2:14 PM), http://www.planetbiometrics.com/article-details/i/5031/desc/yahoo-adds-fingerprint-security-after-massive-hack.

6. *Id.*

from avant-garde trend to everyday reality; passwords are old school, biometrics are new school. For example, almost all of the latest smartphone models come equipped with a built-in fingerprint sensor,[7] and MasterCard is releasing MasterCard Identity Check, a.k.a. "selfie pay," which uses facial recognition for payment authentication.[8] Other biometric identification processes utilize voice authentication or iris scans; there may even be a time when a shopper can use a picture of his or her ear to checkout at a store.[9]

While biometrics are highly advanced and becoming ubiquitous, the use of biometrics poses unique safety and security issues. As a security expert from Kaspersky Lab[10] explained, "[t]he problem with biometrics is that unlike passwords or PIN codes which can be easily modified in the event of compromise, it is impossible to change your fingerprint or iris image . . . Thus if your data is compromised once, it won't be safe to use that authentication method again."[11] Biometric data is easier to obtain than many might think. An investigation by Kasperky Lab into underground cybercrime revealed that there are at least twelve sellers offering skimmers capable of stealing fingerprints, and there are at least three sellers researching devices that could obtain data from a person's iris and palm veins.[12]

Despite the increasing dependency on biometric authentication methods and the developing risks of biometric data breaches, there are few laws governing the protection and storage of biometric data.[13] In the United States, only Texas and Illinois have

---

7. Kate Kochetkova, *Mobile Fingerprint Sensors: More Or Less Secure?*, KASPERSKY LAB (Jan. 21, 2016), https://blog.kaspersky.com/fingerprints-sensors-security/10951.

8. Natasha Lomas, *Mastercard Launches Its 'Selfie Pay' Biometric Authentication App In Europe*, TECHCRUNCH (Oct. 4, 2016), https://techcrunch.com/2016/10/04/mastercard-launches-its-selfie-pay-biometric-authentication-app-in-europe.

9. April Glaser, *Biometrics Are Coming, Along with Serious Security Concerns*, WIRED (Mar. 9, 2016), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns.

10. Kaspersky Lab is the largest privately-owned cybersecurity company. *About Kaspersky Lab*, KASPERSKY LAB, http://usa.kaspersky.com/about-us/company-overview (last visited Feb. 10, 2017).

11. *Biometric Skimmers Are Here: Kaspersky Lab Examine Near-Future Threats To ATMs*, KASPERSKY LAB (Sept. 22, 2016), http://usa.kaspersky.com/about-us/press-center/press-releases/2016/Biometric_skimmers_are_here_Kaspersky_Lab_Examine_Near-Future_Threats_to_ATMs.

12. *Id.*

13. Theodore F. Claypoole & Cameron S. Stoll, *State Forays into the Regulation of Biometric Data*, LAW360 (Nov. 10, 2015, 11:12 AM), http://www.law360.com/articles/724349/state-forays-into-the-regulation-of-biometric-data.

implemented laws that specifically focus on biometric security.[14] In December 2015, the European Commission published the General Data Protection Regulation, which includes regulations on the collection, use, and transfer of biometric data.[15] While these European Union ("EU") regulations may affect companies that deal in a global market, the EU regulations are not binding law in United States courts.[16]

This Note will examine current regulations, open questions, and methods to best regulate biometric data through the lens of individual privacy concerns. Section II will provide an overview of what biometrics are, how biometrics are used, and the risks biometrics pose to security and privacy. Section III will examine existing laws within the United States, case law, and precedent dealing with issues relating to biometrics. Section IV will examine the law in California specifically, and propose legislation to address the concerns and problems raised in this Note.

II. BACKGROUND

A. An Overview of Biometrics

1. What Are Biometrics?

Simply speaking, a biometric is a form of human recognition; to be more specific, a biometric is the "automated technique of measuring a physical characteristic or personal trait of an individual and comparing that characteristic or trait to a database for purposes of recognizing that individual."[17] Biometrics include: physical characteristics and personal traits, such as facial features;

14. Sam Castic, Shea G. Leitch, Aravind Swaminathan & Antony P. Kim, *Biometrics: A Fingerprint for Privacy Compliance, Part I*, ORRICK (Mar. 4, 2016), http://blogs.orrick.com/trustanchor/2016/03/04/biometrics-a-fingerprint-for-privacy-compliance-part-i.

15. Jonathan Millard & Tyler Newby, *EU's General Data Protection Regulation: Sweeping Changes Coming to European and U.S. Companies*, ABA (May 23, 2016), http://apps.americanbar.org/litigation/committees/technology/articles/spring2016-0516-eu-general-data-protection-regulation.html.

16. Although the EU law is not binding within United States courts, American companies may still be subject to suit or penalties of up to four percent of gross revenue for non-compliance with the EU law. *Id.*

17. John D. Woodward, *Biometrics: Identifying Law and Policy Concerns*, *in* BIOMETRICS: PERSONAL IDENTIFICATION IN NETWORKED SOCIETY 385, 387 (Anil Jain et al. eds., 1996).

fingerprints; the retina and iris of the eye, and; veins.[18] There are also auditory biometrics, such a person's voice, and behavioral biometrics, such as a person's gait.[19]

Although biometrics are now experiencing a widespread increase in popularity, making everyday activities appear evermore like a science fiction film, the use of biometrics is not new. For example, fingerprinting can be traced back to China in the fourteenth century.[20] In determining which biometric to use, entities often examine different factors.[21] These include universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention.[22] Uniqueness is considered to be the priority requirement for biometric data, as a biometric system will be able to recognize each user among groups of users based on a person's unique identifiers.[23] "For instance, the DNA of each person is unique and . . . impossible to replicate."[24]

Biometric identification utilizes an intrinsic aspect of a particular human being. Thus, using biometrics can be preferable to other forms of security measures, in light of this "uniqueness" factor.[25] The "chance of two users having the same identification in the biometrics security technology system is nearly zero," ignoring potential counterfeiting efforts.[26]

---

18. *Types of Biometrics*, BIOMETRICS INST., http://www.biometricsinstitute.org/pages/types-of-biometrics.html (last visited Feb. 10, 2017).

19. *Id.*

20. *History of Biometrics*, GLOBALSECURITY.ORG, http://www.globalsecurity.org/security/systems/biometrics-history.html (last updated July 13, 2011).

21. Chien Le, *A Survey of Biometrics Security Systems* (Nov. 28, 2011), http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet.pdf.

22. Uniqueness indicates "how differently and uniquely the biometric system will be able to recognize each user among groups of users." *Id.* Universality "indicates requirements for unique characteristics of each person in the world, which cannot be replicated." *Id.* Permanence deals with whether a characteristic or trait is constant or changes over time. *Id.* Collectability "requires the collection of each characteristic and trait by the system in order to verify their identification." *Id.* Performance "outlines how well the security system works," as determined by accuracy and robustness. *Id.* "The acceptability parameter will choose fields in which biometric technologies are acceptable." *Id.* Circumvention "will decide how easily each characteristic and trait provided by the user can lead to failure during the verification process." *Id.*

23. *Id.*

24. *Id.* However, it is possible to fabricate DNA. Andrew Pollack, *DNA Evidence Can Be Fabricated, Scientists Show*, N.Y. TIMES (Aug. 17, 2009) http://www.nytimes.com/2009/08/18/science/18dna.html.

25. Le, *supra* note 21.

26. *Id.*

Recognition systems that are not based on "an intrinsic aspect of a human being are not always secure."[27] For instance, a recognition system that relies on memory, such as a password, or a tangible object, such as a badge, can be easily compromised, given that passwords can be stolen or forgotten and badges can be lost or duplicated.[28] Because biometrics are unique to individuals, a recognition system based on biometrics is not as easily compromised.[29] "Unlike traditional [recognition systems] which you must either remember or carry with you, biometrics *are* you."[30] However, as discussed below, biometrics can be susceptible to a different range of problems, including theft.

2. How Are Biometrics Used?

a. Government use

The 1990s saw the initial rise of biometric identification, as computers became more advanced.[31] However, in the 1990s the use of biometrics was still mostly limited to law enforcement.[32]

Following the terrorist attacks on September 11, 2001, the use of biometrics in the government and beyond spread rapidly.[33] From 2003 to 2013, the Department of Homeland Security spent over $133 million on biometrics; the FBI expanded its fingerprint database and developed a more sophisticated system using iris scans, palm scans, and facial recognition; and "the U.S. military has collected fingerprints, iris scans, and facial images from millions of Iraqis and Afghans" to help identify rebels.[34] Additionally, "[t]he U.S. Department of Homeland Security has its own system called US-VISIT, for which non-U.S. passport holders are required to submit all 10 fingerprints and a digital photograph before leaving for the

27. John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 101 (1997).

28. *Id.*

29. *Id.*

30. Tim De Chant, *The Boring and Exciting World of Biometrics*, PBS (June 18, 2013), http://www.pbs.org/wgbh/nova/next/tech/biometrics-and-the-future-of-identification.

31. *Id.*

32. *Id.*

33. *Id.*

34. *Id.*

U.S.," and when they enter the U.S., "their biometrics are collected again and compared against a database . . . to verify their identify."[35]

b. Private sector and commercial use

Biometrics are increasingly being used in business organizations, residential and commercial security applications, online banking transactions, electronic devices, and motor vehicles.[36] "As more global financial activity becomes digitally-based," many banks are incorporating the use of biometric technologies into their service platforms.[37] For example, "Bank of America[] customers can use the fingerprint scanner on their mobile phones to sign into the [Bank of America] mobile banking app[lication]."[38] Further improving the accessibility of banking services, Citibank uses voice biometrics authentication.[39] This authentication service automatically identifies a customer while he or she explains an issue to a customer service representative over the phone, eliminating the process of verifying a customer's identity through ID numbers and personal details.[40]

But the use of biometrics extends far beyond the banking industry. Biometric technologies are widespread in the technology sector.[41] For example, Apple introduced Touch ID, a fingerprint sensor, on its iPhone 5S.[42] HTC and Samsung introduced similar technology, which unfortunately resulted in serious security risks, leaving twelve million phone owners vulnerable to hackers and

35. *Id.* This even applies to most visitors entering under the Visa Waiver Program. *US Visit—Entry/Exit System*, IMMIHELP, http://www.immihelp.com/visas/usvisit.html (last visited Feb. 10, 2017).

36. *See Biometrics Technology Market by Technology*, CREDENCE RES. (Apr. 2016), http://www.credenceresearch.com/report/biometrics-technology-market.

37. Bethany Frank, *Five Examples of Biometrics in Banking*, ALACRITI (Feb. 22, 2016), http://www.alacriti.com/biometrics-in-banking.

38. *Id.*

39. *Id.*

40. *Id.*

41. Pierce Ivory, *Understanding Biometric Technology and Biometric Devices*, ENG'RS J. (Apr. 17, 2016), http://www.engineersjournal.ie/2016/04/17/understanding-biometric-technology-and-biometric-devices. ("Biometric technology is commonly used for authenticating individuals before granting access to smartphones, tablets and other electronic devices.").

42. Chenda Ngak, *Apple Announces New Iphone 5S, Iphone 5C, Ios 7 Release Date*, CBS (Sept. 10, 2013, 8:40 PM), http://www.cbsnews.com/news/apple-announces-new-iphone-5s-iphone-5c-ios-7-release-date.

malware.[43] In early June 2011, Facebook unveiled a new feature called "tag suggestions" to all of its users, which uses facial recognition to help identify people in photos uploaded to the site.[44] The legal problems that Facebook's use of facial recognition software pose will be discussed in depth in section three of this note.

B. Privacy Concerns & Policy

With the increasing use of biometrics across both the public and private sectors, consumers have grown more comfortable with using such advanced technology.[45] Despite this comfort level, biometric technologies still pose great risks. Data security breaches are a huge problem for American businesses and consumers.[46] To hackers, any organization is fair game, and companies like Sony, JP Morgan, Target, Ashley Madison, and BlueCross have all been hacked within the past five years.[47] Hacking has even crossed over into the political sphere, as evidenced by hacks into the Democratic National Committee and into Hillary Clinton's campaign emails; many people consider these hacks to be a part of cyberespionage and an information-warfare campaign executed by Russia.[48] Currently, forty-seven states, including California, have enacted Security Breach Notification Laws, which generally require companies to

43. Dave Gershgorn, *Here's How HTC and Samsung's Fingerprint Scanner Was Hacked*, POPULAR SCI. (Aug. 10, 2015), http://www.popsci.com/how-samsung-and-htcs-fingerprint-security-was-hacked.

44. Carmen Aguado, *Facebook or Face Bank?*, 32 LOY. L.A. ENT. L. REV. 187, 188 (2012).

45. A study by the Consumer Technology Association found that 62% of U.S. adults who have used biometric technologies are comfortable with it; 58% of consumers support biometric technologies for altruistic purposes in medical research; and "[m]ore than half of U.S. adults are either very comfortable or comfortable with the use of biometrics in . . . airports and [at] national borders." *Biometric Technology Enjoys Strong Support from Consumers, Says CTA*, BUSINESSWIRE (Mar. 30, 2016, 1:09 PM), http://www.businesswire.com/news/home/20160330006149/en/Biometric-%C2%AD-Technology-%C2%AD- Enjoys-%C2%AD- Strong-%C2%AD- Support-%C2%AD-Consumers-%C2%AD- CTA.

46. By December 2016, there had been an estimated 980 data breaches across the banking, business, educational, government, and healthcare sectors on the year, exposing an estimated 35,233,317 records. *2016 Data Breach Category Summary*, IDENTITY THEFT RES. CTR., at 4 (Dec. 13, 2016), http://www.idtheftcenter.org/images/breach/DataBreachReport_2016.pdf.

47. Claire Groden, *Here's Who's Been Hacked in the Past Two Years*, FORTUNE (Oct. 2, 2015), http://fortune.com/2015/10/02/heres-whos-been-hacked-in-the-past-two-years.

48. Eric Lipton et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0; Tal Kopan & Dan Merica, *What We've Learned From the Hacked Emails of Hillary Clinton's Campaign (So Far)*, CNN (Oct. 18, 2016), http://edition.cnn.com/2016/10/18/politics/hillary-clinton-campaign-email-hack-what-learned.

notify consumers when a breach has occurred.[49] After a breach has occurred, consumers may seek recourse by bringing claims under various legal theories, including violations of the Electronic Communications Privacy Act,[50] the Computer Fraud and Abuse Act,[51] state unfair-competition laws, and common law claims such as breach of contract and invasion of privacy.[52] While the existence of such potential civil remedies and notification laws is imperative to the safety of consumers, it is important to remember that biometric data is inherently different than other kinds of data, and thus, should be treated differently under the law.

Because biometrics contain sensitive, personal information, biometric scanning can implicate its own unique set of privacy concerns. In addition to the identification data obtained, information about a person's health can also be acquired. For example, a fingerprint scan can determine if a person has certain chromosomal disorders, like Down syndrome, Turner syndrome, and Klinefelter syndrome.[53] Unusual fingerprint patterns can also determine certain non-chromosomal disorders, like leukemia, breast cancer, and Rubella syndrome.[54] Additionally, retinal scans can reveal drug or alcohol abuse.[55] Because information on medical histories and lifestyle choices can be gleaned from biometrics, the use of biometrics raises privacy concerns in a way that other personally identifiable information might not.[56]

---

49. *Security Breach Notification Laws*, NAT'L CONF. ST. LEGIS. (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

50. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-22 (West 2012).

51. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2012).

52. ANDREW B. SERWIN, INFORMATION SECURITY AND PRIVACY: A GUIDE TO FEDERAL AND STATE LAW AND COMPLIANCE § 34:2 (West 2016).

53. Woodward, *supra* note 17, at 393.

54. *Id.*

55. Jason Peragallo et al., *Ocular Manifestations of Drug and Alcohol Abuse*, NAT'L CTR. FOR BIOTECHNOLOGY INFO., at 4 (Aug. 22, 2015), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4545665/pdf/nihms716264.pdf.

56. It is important to note that medical records and information have long been entitled to privacy protection, and have even been held to a higher standard of privacy than other information. *See* United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980) ("There can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection. Information about one's body and state of health is a matter which the individual is ordinarily entitled to retain within the private enclave where he may lead a private life. It has been recognized in various contexts that medical records and information stand on a different plane than other relevant material."); *see also* Whalen v. Roe, 429 U.S. 589, 599 (1977) (explaining that

1. History of Privacy Law

The word "privacy" (much like the word "biometrics") is absent from the text of the United States Constitution.[57] However, the right to information privacy[58] can be read into the Constitution.[59] For example, the First Amendment protects freedom of speech, press, and association;[60] the Third Amendment prohibits the quartering of soldiers in one's home;[61] the Fourth Amendment provides for the right to be free from unreasonable searches and seizures;[62] and the Fifth Amendment protects against self-incrimination.[63] In 1890, Samuel D. Warren and Louis D. Brandeis penned *The Right to Privacy*, which articulated their view of privacy as the "right to be let alone."[64] Later, this law review article helped develop the common law action for invasion of privacy.[65] However, "the right to be let alone" is vague, and "legally, it offers no guidance at all. Coveting an indefinable right is one thing; enforcing it in a court of law is another."[66]

Yet, the Constitution's privacy protections are usually not implicated in regard to biometrics because most biometric scanning

---

the Constitution protects "the individual interest in avoiding disclosure of personal matters" including medical information); *but see*, Doe v. Att'y Gen. of United States, 941 F.2d 780, 796 (9th Cir. 1991), *disapproved by* Lane v. Pena, 518 U.S. 187 (1996) ("[T]he privacy protection afforded medical information is not absolute; rather, it is a conditional right which may be infringed upon a showing of proper governmental interest."); NASA v. Nelson, 562 U.S. 134, 159 (2011) (holding the government's inquiries into an employee's background did not violate a constitutional right to informational privacy, because the challenged inquiries were reasonable and the Privacy Act of 1974 provided safeguards against disclosure).

57. *See* U.S. CONST.

58. Information privacy, as discussed in this article, deals with restricted access; it refers to a person keeping his or her mental state or personal information private from others. Information privacy is distinct from decisional privacy. Decisional privacy refers to freedom from outside interference in decision-making—governmental or otherwise—in appropriately private affairs, including such matters as one's sexual orientation, or decisions regarding abortion. *Privacy, Private Choice, and Social Contract Theory* 461–91 (U. of Pa. Law Sch. Faculty Scholarship, Paper No. 1337), http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2337&context=faculty_scholarship.

59. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) ("[S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy.").

60. U.S. CONST. amend. I.

61. U.S. CONST. amend. III.

62. U.S. CONST. amend. IV.

63. U.S. CONST. amend. V.

64. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

65. *See* Diamond Shamrock Ref. & Mktg. Co. v. Mendez, 844 S.W.2d 198, 203 (Tex. 1992).

66. ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY xiv (1995).

results from use in private sectors, in which users voluntarily give up information.[67] Thus, in order to find laws dealing with an individual's right to privacy when biometric data is freely given, one must turn to state law.

2. Existing Law and Guidelines

The United States' "nationwide privacy law regime is based on the sectoral approach."[68] Thus, many different sources of privacy laws include biometric data. Laws that affect the use of biometric information can be broken down into two general categories: (1) broad privacy laws that include biometric information in the definition of personal information, and; (2) laws that specifically address the use of biometric identifiers.[69]

For example, "various industry-specific laws also govern private and public actor[s'] use of individual[s'] biometric information in their governance of financial institutions, educational institutions, commercial entities, and health-care providers."[70] However, despite broad coverage in many sectors of privacy law, falling under this general umbrella may not provide adequate avenues of protection or recovery for the unique privacy concern that biometric data poses.

Many state laws have incorporated biometric information into definitions of personal information. For example, Iowa's Personal Information Security Breach Protection law requires that a consumer be notified when a breach of personal information occurs, including

67. Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (explaining that the Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"); Laurence H. Tribe, Professor of Law, Harvard Law School, Keynote Address at the First Conference on Computer, Freedom & Privacy: The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier (Mar. 26, 1991), transcript available at http://groups.csail.mit.edu/mac/classes/6.805/articles/tribe-constitution.txt) ("[T]he Constitution, with the sole exception of the Thirteenth Amendment prohibiting slavery, regulates action by the government rather than the conduct of private individuals and groups.").

68. Ted Claypoole & Cameron Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric Information*, AM. B. ASS'N (May 2, 2016), http://www.americanbar.org /publications/blt/2016/05/08_claypoole.html.

69. *Id.*

70. *Id.* While there is a vast body of law that governs a public actor's use of biometric information, this note only focuses on laws that govern a private actor's use of biometric information, focusing on the protections that are or are not afforded to biometric data that is given freely for private use.

a breach of "unique biometric data."[71] Nebraska includes biometric information within its Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006.[72] Wisconsin includes biometric data in its criminal identity-theft statute.[73]

Overall, many states, like Iowa, Nebraska, and Wisconsin, do identify biometric information as personal information. But, some states, like South Carolina, define "personal identifying information" as a person's name as well as "other numbers, passwords, or information which may be used to access a person's financial resources, numbers, or information issued by a governmental or regulatory entity that uniquely will identify an individual or an individual's financial resources."[74] As discussed above, a fingerprint will "uniquely . . . identify an individual" and can be used to "access a person's financial resources," yet this biometric identifier is not explicitly recognized under South Carolina law.[75] Thus, while "[m]ost states' data breach notification laws will govern unauthorized access to residents' biometric information . . ., such inclusion may be vague, and not specifically identify biometric information."[76]

3. Biometric Specific Laws

a. Illinois

The first state law to specifically address businesses' collection of biometric data was the Illinois Biometric Information Privacy Act ("BIPA") in 2008.[77] Recognizing that the use of biometrics is growing in the business and security screening sectors, and that biometrics are unlike other unique personal identifiers, Illinois

71. IOWA CODE ANN. § 715C.1(11)(a)(5) (West 2014) (defining personal information to include "unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data").

72. NEB. REV. STAT. ANN. § 87-802(5)(a)(v) (West 2016) (defining personal information as including "[u]nique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation").

73. WIS. STAT. ANN. § 943.201(1)(b)(13) (West 2017) (defining biometric data as "including fingerprint, voice print, retina or iris image, or any other unique physical representation").

74. S.C. CODE ANN. § 16-13-510(D) (2003).

75. *See id.*

76. Claypoole & Stoll, *supra* note 68.

77. *Id.*

enacted BIPA for the welfare, security, and safety of its citizens.[78] Importantly, BIPA clearly defines a "biometric identifier," in relevant part, as:

> a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.[79]

Overall, BIPA can be broken down into five main elements. The law: (1) requires informed consent for collection; (2) prohibits profiting from biometric data; (3) allows a limited right to disclose; (4) creates obligations for the protection of biometric data, and; (5) creates a private right of action.[80]

First, BIPA prohibits a private entity from collecting, capturing, purchasing, receiving, or otherwise obtaining a person's biometric information, unless it: (1) informs the person, in writing, that the biometric information is being collected and stored; (2) informs the person, in writing, of the specific purpose and length of term for which biometric information is being collected, stored, and used, and; (3) receives the person's written consent.[81] The written policy must state the business's retention schedule for data and rules for destruction of the biometric data.[82] Additionally, a business may not store biometric data after the initial purpose for collecting the data has been satisfied, or after a period of three years since the person's interaction with the business, whichever occurs first.[83] While BIPA requires a written release, the form and content of the written release is not delineated.[84]

Second, BIPA mandates that "[n]o private entity in possession of a biometric identifier or biometric information may sell, lease,

78. 740 ILL. COMP. STAT. ANN. 14/5 (West 2008).
79. 740 ILL. COMP. STAT. ANN. 14/10 (West 2008).
80. 740 ILL. COMP. STAT. ANN. 14/15–14/20 (West 2008).
81. 740 ILL. COMP. STAT. ANN. 14/15(b) (West 2008).
82. 740 ILL. COMP. STAT. ANN. 14/15(a) (West 2008).
83. *Id.*
84. Claypoole & Stoll, *supra* note 68 (explaining that "click-wraps," which require consumers to press an "accept" button, will likely meet BIPA's requirements, but "browse-wrap" agreements, which do not require affirmative acceptance, likely will not meet BIPA's requirements).

trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information."[85]

Third, BIPA limits the disclosure or dissemination of a person's biometric information.[86] Biometric information may not be disclosed unless: the subject consents; the disclosure completes a financial transaction requested by the individual; the disclosure is required by Illinois law, municipal ordinance, or federal law; or the disclosure is required by a valid warrant or subpoena.[87]

Fourth, BIPA requires that a private entity in possession of biometric information use the reasonable standard of care within its industry to store, transmit, and protect from the disclosure of the biometric information.[88] Additionally, BIPA mandates that a business use the same or more protective measures with respect to biometric data as it does with respect to other confidential or sensitive information.[89]

Fifth, any person harmed by a violation of BIPA may recover against a private entity.[90] For negligent violations, a person can recover liquidated damages of $1,000, or actual damages, whichever is greater.[91] For intentional or reckless violations, a person can recover liquidated damages of $5,000, or actual damages, whichever is greater.[92] Additionally, a person can recover attorneys' fees and costs, and may be entitled to other monetary or injunctive relief.[93]

Given BIPA's private right of action, the potential for monetary sanctions and injunctive relief under the Act, its consent requirement, its prohibitions on profiting from data, its conditions for disclosure, and its requirements for storage and protection, BIPA is often considered America's strongest biometric privacy law.[94] And, as

85. 740 ILL. COMP. STAT. ANN. 14/15(c) (West 2008). However, BIPA is "silent as to how direct the causal link must be between the profit and the data to qualify as a violation of the provision." Claypoole & Stoll, *supra* note 68.

86. 740 ILL. COMP. STAT. ANN. 14/15(d) (West 2008).

87. *Id.*

88. 740 ILL. COMP. STAT. ANN. 14/15(e) (West 2008).

89. *Id.*

90. 740 ILL. COMP. STAT. ANN. 14/20 (West 2016).

91. *Id.*

92. *Id.*

93. *Id.*

94. *See* Russell Brandom, *Someone's Trying to Gut America's Strongest Biometric Privacy Law*, VERGE (May 27, 2016, 8:27 AM), http://www.theverge.com/2016/5/27/11794512/facial-recognition-law-illinois-facebook-google-snapchat.

discussed below, BIPA is causing many problems for large technology companies.

b. Texas

Following shortly after BIPA, Texas enacted biometric laws in 2009, contained in Section 503.001 of the Texas Business and Commercial Code (the "Texas law").[95] The Texas law defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[96] Similar to BIPA, the Texas law requires an individual's consent before a business may capture a person's biometric identifier, limits the time a business may store biometric data, and requires businesses to store, transmit, and protect biometric data in the same or a more protective manner as it would other confidential information.[97] However, while similar in some ways, the Texas law "lacks BIPA's heft and scope."[98] For example, the Texas law allows a business to "sell, lease, or otherwise disclose the biometric identifier to another person" under limited circumstances, and caps the civil penalty at $25,000 for each violation.[99]

III. ANALYSIS

A. Case Law and Precedent

In June 2015, Brian Norberg filed a class action lawsuit against Shutterfly, a popular online photo book service.[100] The suit, filed in federal court in Illinois, alleged that Shutterfly violated BIPA by collecting and storing "millions of 'face templates' (or 'face prints')—highly detailed geometric maps of the face—from millions of individuals, many thousands of whom [were] non Shutterfly

95. Claypoole & Stoll, *supra* note 68.

96. TEX. BUS. & COM. CODE § 503.001(a) (West 2015).

97. TEX. BUS. & COM. CODE § 503.001(a)–(c) (West 2015).

98. Claypoole & Stoll, *supra* note 13.

99. TEX. BUS. & COM. CODE § 503.001 (c)–(d) (West 2015). The Texas law allows for sale and disclosure in limited circumstances, including in the event of the individual's disappearance or death, to complete a financial transaction requested or authorized by the individual, as required by statute, or in response to a warrant. *Id.* at (c).

100. Jeff John Roberts, *Shutterfly Hit With Privacy Suit Over "Faceprints," Use of Photos*, FORTUNE (June 18, 2015, 12:19 PM), http://fortune.com/2015/06/18/shutterfly-lawsuit-facial-recognition.

users."[101] Once a picture was uploaded to Shutterfly, Norberg alleged that Shutterfly's "sophisticated facial recognition technology create[d] a template for each face" and then suggested to tag a name already associated with that face.[102] Norberg alleged that a Shutterfly user uploaded a picture of Norberg and tagged Norberg in the photo.[103] For each photo of Norberg uploaded subsequently, Norberg alleges that Shutterfly automatically suggested that the user tag Norberg.[104] Norberg further alleged that he never created a Shutterfly account and never used Shutterfly, and thus, never gave his consent or permission, written or otherwise, for Shutterfly to use his biometric information.[105] Shutterfly filed a Motion to Dismiss, arguing that Norberg failed to state a claim under BIPA, and the court denied Shutterfly's motion.[106] However, in April 2016, before a class was certified, both parties moved to dismiss the case after reaching an undisclosed settlement.[107]

In 2015, Adam Pezen, Carlo Licata, and Nimesh Patel, separately sued Facebook, alleging that Facebook was collecting biometric data from people tagged in photos posted by other users in violation of BIPA.[108] For reference, Facebook reported in 2010 that "its users had applied more than 100 millions 'tags' to photos uploaded to its site."[109] These cases were combined and transferred to a federal district court in California.[110] Facebook then filed a Motion to Dismiss, arguing that a California choice-of-law provision in Facebook's user agreement precluded suing on an Illinois statute,

101. Complaint at 3, Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103 (N.D. Ill. 2015) (No.1:15-cv-05351).

102. *Id.* at 8.

103. *Id.* at 9.

104. *Id.* at 9–10.

105. *Id.* at 10.

106. Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1104 (N.D. Ill. 2015).

107. Kim Janssen, *Shutterfly Settles Facial Recognition Lawsuit with Man who Claimed Privacy Violation*, CHI. TRIB. (Apr. 12, 2016 2:57 PM), http://www.chicagotribune.com/business/ct-facial-recognition-lawsuit-0413-biz-20160412-story.html.

108. Dawn Rhodes, *California Judge: Illinois Facebook 'Tagging' Lawsuit Can Proceed*, CHI. TRIB. (May 10, 2016 3:28 PM), http://www.chicagotribune.com/news/local/breaking/ct-facebook-lawsuit-20160510-story.html.

109. Stephanie Grimoldby, *Illinois Facial Recognition Law Leads to Wave of Class Actions Against Facebook, Others*, FORBES (July 5, 2016, 6:00 AM), http://www.forbes.com/sites/legalnewsline/2016/07/05/il-facial-recognition-law-leads-to-wave-of-class-actions-against-facebook-others/#1a3f3fc04e56.

110. *Id.*

and that the plaintiffs failed to state a claim under BIPA.[111] The court held that although a valid choice-of-law agreement was formed between the three plaintiffs and Facebook, it would not be enforced.[112] Following Section 187 of the Restatement (Second) of Conflict of Laws, the court explained that "if California law [was] applied, the Illinois policy of protecting its citizens' privacy interests in their biometric data, especially in the context of dealing with 'major national corporations' like Facebook, would be written out of existence."[113] Additionally, the court held that plaintiffs sufficiently stated a claim under BIPA, finding unpersuasive Facebook's "contention that the statute categorically excludes from its scope all information involving photographs."[114] The court, reading the statute as a whole, found that photographs are "better understood to mean paper prints of photographs, not digitized images stored as a computer file and uploaded to the Internet," and refused to "read the statute to categorically exclude from its scope all data collection processes that use images."[115]

Although this ruling is not a final decision, it does pose significant threats to social media sites and other businesses using facial recognition software and other biometric identifiers. Additionally, another suit was brought against Facebook in response to its tagging feature, but was dismissed for lack of personal jurisdiction.[116] Google is now facing a similar suit in the United States District Court for the Northern District of Illinois.[117]

If the class action lawsuits against Facebook and Google succeed, the companies could be forced "to pay millions of dollars in damages and, in what would likely be a greater nuisance, force them to change their policies around how they use faces."[118] In response, it is rumored that Facebook and Google were behind lobbying efforts

111. *In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1158 (N.D. Cal. 2016).

112. *Id.* at 1168–70.

113. *Id.* at 1169.

114. *Id.* at 1171.

115. *Id.*

116. Gullen v. Facebook.com, Inc., No. 15 C 7681, 2016 WL 245910 (N.D. Ill. Jan. 21, 2016).

117. Complaint at 1, Rivera v. Google Inc., No. 16-02714 (N.D. Ill. March 1, 2016).

118. Jeff John Roberts, *Facebook and Google Really Want to Kill This Face-Scanning Law*, FORTUNE (June 30, 2016) http://fortune.com/2016/06/30/facebook-google-facial-recognition-lawsuits.

in May 2016 to persuade lawmakers to amend "the legal definitions of the terms 'photographs' and 'scan' so as to exclude activities related to digital photo 'tagging.'"[119] However, the proposed amendment was not passed before the Illinois legislature ended its session.[120]

While the above cases focus on facial recognition, that is not the only biometric identifier subject to litigation.

Adina McCollough recently filed suit against Smarte Carte in the Northern District of Illinois, alleging the company had violated BIPA.[121] In addition to rental services for luggage carts and strollers, Smarte Carte owns and operates electronic locker rentals.[122] A renter may open a Smarte Carte locker by using his or her fingerprint as a key.[123] To use one of Smarte Carte's lockers, a renter provides his or her fingerprint on a centrally located scanner and is assigned a specific locker; after placing items in the locker and shutting the door, the locker is secured; upon return, the customer provides another fingerprint scan, which, when matched to the initial scan, opens the locker.[124] On five occasions, McCollough used Smarte Carte's electronic lockers.[125] McCollough alleged that Smarte Carte violated BIPA, as it failed to obtain its customers' "written consent to record, collect, obtain or store" fingerprint data and to disclose the duration of data storage.[126]

The court found that, although Smarte Carte's policy was a technical violation of BIPA, McCollough lacked standing, as she failed to allege sufficient facts to show that she was "a person 'aggrieved *by* a violation' of BIPA."[127] The court explained that McCollough must have realized that the system would store her fingerprint for a period of time, given that her fingerprint was the key to unlocking the locker.[128] The court further questioned what "concrete harm" McCollough could suffer from Smarte Carte merely

119. Jeff John Roberts, *Push to Weaken Face Recognition Law Falls Short, for Now*, FORTUNE (May 31, 2016, 7:46 PM), http://fortune.com/2016/05/31/biometric-law-change/.
120. *Id.*
121. McCollough v. Smarte Carte, Inc., 2016 WL 4077108, at *1 (N.D. Ill. Aug. 1, 2016).
122. *Id.*
123. *Id.*
124. *Id.*
125. *Id.*
126. *Id.*
127. *Id.* at *4.
128. *Id.* at *3.

storing her "fingerprint data for longer than the rental period."[129] However, the court did note that unauthorized disclosure could constitute a concrete injury, sufficient to establish standing.[130]

With the Facebook and Google litigations still pending in court, and many cases being dismissed on procedural grounds, the future of privacy with respect to facial recognition technology and other biometrics remains largely unknown.[131]

B. California Legislation

The California Constitution states: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."[132] To protect this inalienable right of privacy, existing California law requires that a business owning, licensing, or maintaining personal information about a California resident implement and maintain "reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[133] For the purposes of privacy, California defines "personal information" as:

> (A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
>
> (i) Social security number.
>
> (ii) Driver's license number or California identification card number.
>
> (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
>
> (iv) Medical information.

---

129. *Id.* at *3–*4.

130. *Id.* at *4–*5.

131. Roberts, *supra* note 118 ("Privacy regulators in other countries, including Canada and many in Europe, have introduced restrictions on the use of facial recognition technology. But for now, it remains largely unregulated in the United States.").

132. CAL. CONST. art. I, § 1 (2016).

133. CAL. CIV. CODE § 1798.81.5(b) (West 2016).

(v) Health insurance information.

(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.[134]

However, "[p]ersonal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."[135] This definition of personal information was amended in July 2015, in Assembly Bill 1541 ("A.B. 1541"), to include "health insurance information . . . and a username or email address combined with a password or security question and answer for access to an online account."[136] While these updates to the definition of personal information better protect California citizens and help address some privacy concerns that technological advances pose,[137] more expansive changes failed. [138] Prior to the close of the 2015–2016 legislative session, an amended Assembly Bill 83 ("A.B. 83") did not pass.[139]

Assemblyman Mike Gatto (D, Glendale) amended A.B. 83, and stated that the "amendments reflect a compromise he negotiated for two years with business and privacy groups that still accomplishes his intent to set standards for protecting personal data where none now exist."[140] A.B. 83 would have expanded data security requirements for businesses that maintain personal information of California residents.[141] Notably, A.B. 83 extended the definition of personal information to include geolocation and biometric information and limited the definition by not including any "publicly

134. CAL. CIV. CODE § 1798.81.5(d)(1) (West 2016).

135. CAL. CIV. CODE § 1798.81.5(d)(4) (West 2016).

136. Assemb.B. 1541, 2015–2016 Leg., Reg. Sess. (Cal. 2015).

137. *See* Sanjay Nangia & Bryan Thompson, *Getting More Personal: California Amends Data Security Law*, DAVIS WRIGHT & TREMAINE (July 29, 2015), http://www.privsecblog.com/2015/07/articles/policy-regulatory-positioning/getting-more-personal-california-amends-data-security-law.

138. Jeffrey Neuburger, *California Legislature Nearing Final Debate of Biometric and Geolocation Data Security Bill*, PROSKAUER ROSE LLP: NEW MEDIA AND TECH. L. BLOG (Aug. 24, 2016), http://newmedialaw.proskauer.com/2016/08/24/california-legislature-nearing-final-debate-of-biometric-and-geolocation-data-security-bill.

139. Assemb.B. 83, 2015-2016 Leg., Reg. Sess. (Cal. 2015).

140. Laura Mahoney, *California Bill Would Add Security Standards to Data Breach Law*, BLOOMBERG L. (Aug. 22, 2016), https://bol.bna.com/california-bill-would-add-security-standards-to-data-breach-law.

141. Assemb.B. 83, 2015–2016 Leg., Reg. Sess. (Cal. 2015).

available information that is lawfully made available to the general public."[142]

Geolocation information means location data generated "by a consumer device capable of connecting to the Internet that directly identifies the precise physical location of the identified individual at particular times and that is compiled and retained," excluding information used for 911 emergency purposes.[143] For example, this "would apply to data gathered by transportation network companies such as Uber Technologies Inc. and Lyft Inc., exercise trackers from Fitbit Inc., and the Internet of Things."[144] A.B. 8 defines biometric information as "data generated by automatic measurements of an individual's fingerprint, voice print, eye retinas or irises, identifying DNA information, or unique facial characteristics, which are used by the owner or licensee to uniquely authenticate an individual's identity."[145] The change to exclude personal information made lawfully available to the general public "could potentially encompass a host of personal data published on the web," which is significantly broader than the current definition.[146] Unlike BIPA and the Texas law, A.B. 83 does not include specific penalties, but as indicated by assemblyman Gatto, "enforcement would happen in one of three ways: through the California Attorney General, through the civil suits under Business and Professions Code section 17200 that appl[y] to unfair competition, and [through] civil suits for negligence."[147]

The success of A.B. 1541 and failure of A.B. 83 highlight the difficult position legislators face when attempting to protect consumers, negotiate with businesses, and anticipate upcoming technological advances. Given that these interests are often in competition, striking a balance will be very difficult.

142. Assemb.B. 83(d)(2)–(3), (6), 2015–16 Leg., Reg. Sess. (Cal. 2015).

143. Assemb.B. 83(d)(2), 2015–2016 Leg., Reg. Sess. (Cal. 2015).

144. Mahoney, *supra* note 140.

145. Assemb.B. 83(d)(3), 2015–2016 Leg., Reg. Sess. (Cal. 2015).

146. Jeffrey Neuburger, *California Legislature Nearing Final Debate of Biometric and Geolocation Data Security Bill*, PROSKAUER ROSE LLP: NEW MEDIA AND TECH. L. BLOG (Aug. 24, 2016), http://newmedialaw.proskauer.com/2016/08/24/california-legislature-nearing-final-debate-of-biometric-and-geolocation-data-security-bill/.

147. Mahoney, *supra* note 140.

C. Proposal

California law does include some protections for its citizens' information. For example, California has a data breach notice law that requires government agencies and businesses to notify any California resident "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[148] However, the California legislature must pass more comprehensive privacy laws that deal specifically with biometric information to keep Californians safe.

1. Definitions

California must recognize the increase of biometrics in today's world and, at a minimum, define biometric information in its statutory framework. By incorporating biometric information explicitly in law, California can help to better protect its citizens from the problems of the present, and the crimes of the future. The definition of biometric information proposed in A.B. 83 is an adequate definition that fairly circumscribes the various biometric identifiers currently available to consumers. However, some changes should be made. For example, the phrase "publicly available information that is lawfully made available to the general public" is very vague, leaving it unclear what personal information would actually be protected.[149] Such uncertainty in the law has great potential to leave citizens unprotected, as companies would likely be unsure of which information is made lawfully available to the general public.

Thus, any future legislation should implement specific definitions and should give clear examples of what information is considered a biometric identifier. The definition should explicitly include such things as: a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. In addition, legislation should give examples of what is not included as a biometric identifier, such as writing samples and physical descriptions. Legislation should also exclude biological samples, fitness trackers/wearables, and medical information.[150]

148. CAL. CIV. CODE § 1798.29 (West 2009).

149. *See generally* Assemb.B. 83(d)(3), 2015–2016 Leg., Reg. Sess. (Cal. 2015).

150. Because much of this information is already governed by HIPAA, any proposed legislation should be limited to true biometric identifiers. *See generally Privacy and Security*,

Perhaps most importantly, legislation should make it clear that only analog, not digital, photographs are not covered by biometric data law; in other words, a picture on Facebook would be subject to any California law on biometrics. Given the concerted campaign detailed above to change the definition of BIPA to exclude digital photographs, it is of the utmost importance that any California legislation make it clear which kinds of photographs are covered under biometric law. The distinction between analog and digital is a common occurrence in many statutory schemes. For example, copyright law, as embodied in the United States Code, was supplemented by the Digital Millennium Copyright Act in 1998.[151] Distinguishing analog from digital content in the law is justified, given that digital content is subject to "perfect replication and easy distribution."[152] The differences in nature between analog and digital content make it is easier to disseminate and misuse digital material. With the increasing opportunity to misuse digital content, a prudent legislature would treat digital content differently than its analog counterpart. It is true that large companies like Facebook or Google might be opposed to the California legislature making digital photography subject to any biometric law. However, the legislature should place the privacy and security of its citizens over big business interest and make this distinction between analog and digital content explicit within the law.

2. Storage and Safety

In dealing with regulating the storage, transfer, and protection of biometric data, California can look to Illinois's and Texas's examples.[153] Following these models, California should place restrictions on the collection of biometric data. Primarily, an individual's consent should be required prior to data being stored or shared. However, it is prudent to allow private entities to circumvent this requirement for consent pursuant to a warrant or subpoena, or if required by law.

HEALTH IT, https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security (last updated Mar. 21, 2014).

151. *Compare* 17 U.S.C. §§ 101–1332, *with* Digital Millennium Copyright Act of 1998, 112 Stat. 2860 (1998).

152. Jude C. Umeh, THE WORLD BEYOND DIGITAL RIGHTS MANAGEMENT 92 (2007).

153. 740 ILL. COMP. STAT. ANN. 14/1 (West 2008); TEX. BUS. & COM. CODE § 503.001 (West 2015).

Additionally, because biometric information is unique to each individual, California law should mandate that businesses only use collected data when it is connected or relevant to the stated purpose of collection. Because biometric information cannot be changed, unlike a social security number or password, once biometric information is acquired by an unauthorized source, it leaves an individual particularly vulnerable. Therefore, biometric information should be handled with extreme caution and used only in limited circumstances.

Like under BIPA, under California law businesses should be required to provide written notice of the purpose and length for which biometric information is collected, stored, or used. Without placing limitations on the use and storage of biometric information, a consumer faces the risk of his or her data being used or sold for purposes beyond the purview of collection. For example, with increasing amounts of biometric data being stored across various platforms, a third party could buy biometric and other data from companies to potentially create a full profile of a consumer. Biometric information is valuable to companies, which could easily buy data, and to thieves, who could easily steal data. Many organizations and companies have recently come under attack of ransomeware, which is "a type of malware that severely restricts access to a computer, device or file until a ransom is paid by the user."[154] If companies can readily acquire a consumer's biometric information, it leaves more consumers and more information vulnerable to attack. Therefore, legislation should require that companies acquiring biometric data inform consumers of the reason for acquiring such data and only store such data for the period of time necessary to accomplish the stated directive.

Moreover, any legislation should place a standard on how companies transmit and store information. Given that data is vulnerable to being hacked at each of these stages, companies should be required to safeguard information. Biometric information should be treated similarly to medical information, given the sensitive, personal nature of both kinds of information. For example, HIPAA requires end-to-end encryption to secure the confidential

154. *Ransomware - Definition, Prevention and Removal*, KASPERSKY LAB, https://usa.kaspersky.com/internet-security-center/definitions/ransomware#.WIl3W7GZPfY (last visited Feb. 10, 2017).

transmission of information, and demands an end-to-end solution to ensure that data remains confidential and secure between a message sender and the intended recipient, preventing unauthorized access or loss of information.[155] Following the example set forth by HIPAA, end-to-end encryption should be the standard for transmission of biometrics information. While end-to-end encryption does not guarantee that information will not be accessed without authorization, it does reduce that risk.[156] Beyond this standard, any legislation should be careful to exclude complex technological requirements for how to deal with biometric data and information. This is because technological advances happen far more rapidly than legal change. If legislation included a specific technological requirement, that technological requirement would likely be phased out of use and replaced by a more advanced technique before the legislation was ever passed. Thus, any legislation should require that a company abide by the best practices in the industry. By requiring companies to maintain industry best practices, the law would ensure that companies use up-to-date technology, and would place the burden on companies to best protect their consumers.

3. Enforcement

California should create a private right of action to allow private individuals to sue for breaches of a California biometrics law. This would allow consumers to recover liquidated or statutory damages. Unlike A.B. 83, which left enforcement to other California statutes,[157] creating a private right action would allow Californians more protection over their biometric information by allowing citizens to enforce the regulations surrounding biometric data.

Alternatively, California could create an agency that would handle enforcement. The agency approach is advantageous because it creates a coherent body of law. Without an agency, different courts could form different rules or models of enforcement when

155. "To avoid a HIPAA violation and reduce the probability of a data breach, [electronic personal health information] should only be transmitted via a secure channel with end to end encryption." *Mobile Data Security and HIPAA Compliance*, HIPAA J., http://www.hipaajournal.com/mobile-data-security-and-hipaa-compliance (last visited Feb. 10, 2017).

156. *See* Andy Greenberg, *Hacker Lexicon: What Is End-to-End Encryption?*, WIRED (Nov. 25, 2014, 9:00 AM), https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.

157. Mahoney, *supra* note 140.

interpreting the law. However, creating a wholly new agency would significantly increase costs to taxpayers. Furthermore, to add the task of prosecuting biometric law violations on an agency already in existence would likely be too taxing on any existing agency. Accordingly, an agency approach is likely not the most efficient route for enforcement.

In sum, creating a private right of action best addresses the harm that such violations cause. Because a consumer is personally violated when information is stolen or is taken without authorization, consumers will likely have better redress if they can spearhead their own litigation, rather than having to rely on an agency to protect them. Additionally, California could implement criminal penalties for repeat offenders and for companies that traffic in devices that allow a user to steal, mimic, or manipulate a person's biometric information.[158]

4. Privacy by Design

While creating legislation is certainly an important part of protecting a citizen's right to privacy in his or her own biometric information, legislation will likely not provide a complete solution. The concept of Privacy by Design addresses this problem by "advanc[ing] the view that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation."[159] Privacy by Design assesses the privacy implications of a technology or practice before it is designed, making privacy an "an essential component of the solution being delivered: it anticipates and prevents privacy invasive events before they can happen."[160] By building privacy into the design of a system

158. Although BIPA and the Texas law do not have a criminal sanctions component, other areas of law, such as copyright law, do include criminal sanctions. For a discussion on the economic effects of criminal prosecution for copyright infringement, see Christopher Buccafusco & Jonathan S. Masur, *Innovation and Incarceration: An Economic Analysis of Criminal Intellectual Property Law* 87 S. CAL. L. REV. 275, 317 (2013).

159. IPC TECHNICAL REPORT, PRIVACY BY DESIGN SOLUTIONS FOR BIOMETRIC ONE-TO-MANY IDENTIFICATION SYSTEMS, INFO. & PRIAVCY COMM'R ONT. 4 (June 2014), https://www.ipc.on.ca/wp-content/uploads/2014/06/pbd-solutions-biometric.pdf.

160. Marie Shroff, N.Z. Privacy Comm'r, Address at the Biometrics Inst. of N.Z. Conf.: Protecting Biometric Data: Privacy By Design (Mar. 26, 2010, 10:29 AM), (transcript available at https://privacy.org.nz/news-and-publications/speeches-and-presentations/protecting-biometric-data-privacy-by-design).

or technology, Privacy by Design can bridge the gap that legislation cannot adequately address.

For example, a person's fingerprint can be replicated from a photograph.[161] So, think twice before posting a photograph of an individual gesturing with a peace sign. Once someone's fingerprint has been stolen or is being used for unauthorized purposes, legislation could provide a person with a means to sue in court, and recover damages. But Privacy by Design aims to avoid this by, for example, advancing the technology of the camera that takes the photograph. Ideally, one day, there will be a camera smart enough to blur parts of the photograph, so that it does not store a person's fingerprint. By building such privacy-focused features into technology, it is less likely that biometrics can be misused. "To maintain customer confidence, and to remain the customer's choice, it is important to protect [personal] information. Good privacy practices are good business."[162] Hopefully businesses and the legislature can work together to protect consumers before and after problems with biometric information occur.

IV. CONCLUSION

In today's increasingly global and technological world, individuals' privacy and security concerns have grown exponentially. In response, lawmakers (both internationally and within the United States) have initiated legislative changes. However, as the above cases and the attempted changes to BIPA indicate, the attempts of lawmakers are facing extreme resistance from some of today's most powerful technological companies. With technological advances moving at a greater rate of change than the law, it is unclear how effective the new laws are at protecting consumers and citizens.

In order to protect its citizens, states are shifting from laws that include some form of biometric information as part of the definition of personal information to laws that specifically address biometric information. This shift is increasingly important as biometric technology starts to be used in nearly every sphere of today's business, technology, and government sectors.

161. Zoe Kleinman, *Politician's Fingerprint 'Cloned From Photos' by Hacker*, BBC (Dec. 29, 2014), http://www.bbc.com/news/technology-30623611.

162. Shroff, *supra* note 160.

Given the uniqueness and specificity of biometric information, California needs to pass laws that protect its citizens. By incorporating the above measures and enacting a biometrics-specific privacy law, the legislature would better protect Californians and provide corporations with more guidance on how to best transact business with an individual's privacy in mind. The failure of A.B. 83 shows the hardship the California legislature will face in drafting a balanced law that protects California citizens from potential abuses of future technology while still making it feasible for companies to conduct the cutting-edge business of today. Yet if California fails to strike this balance, both citizens and companies will remain unprotected.